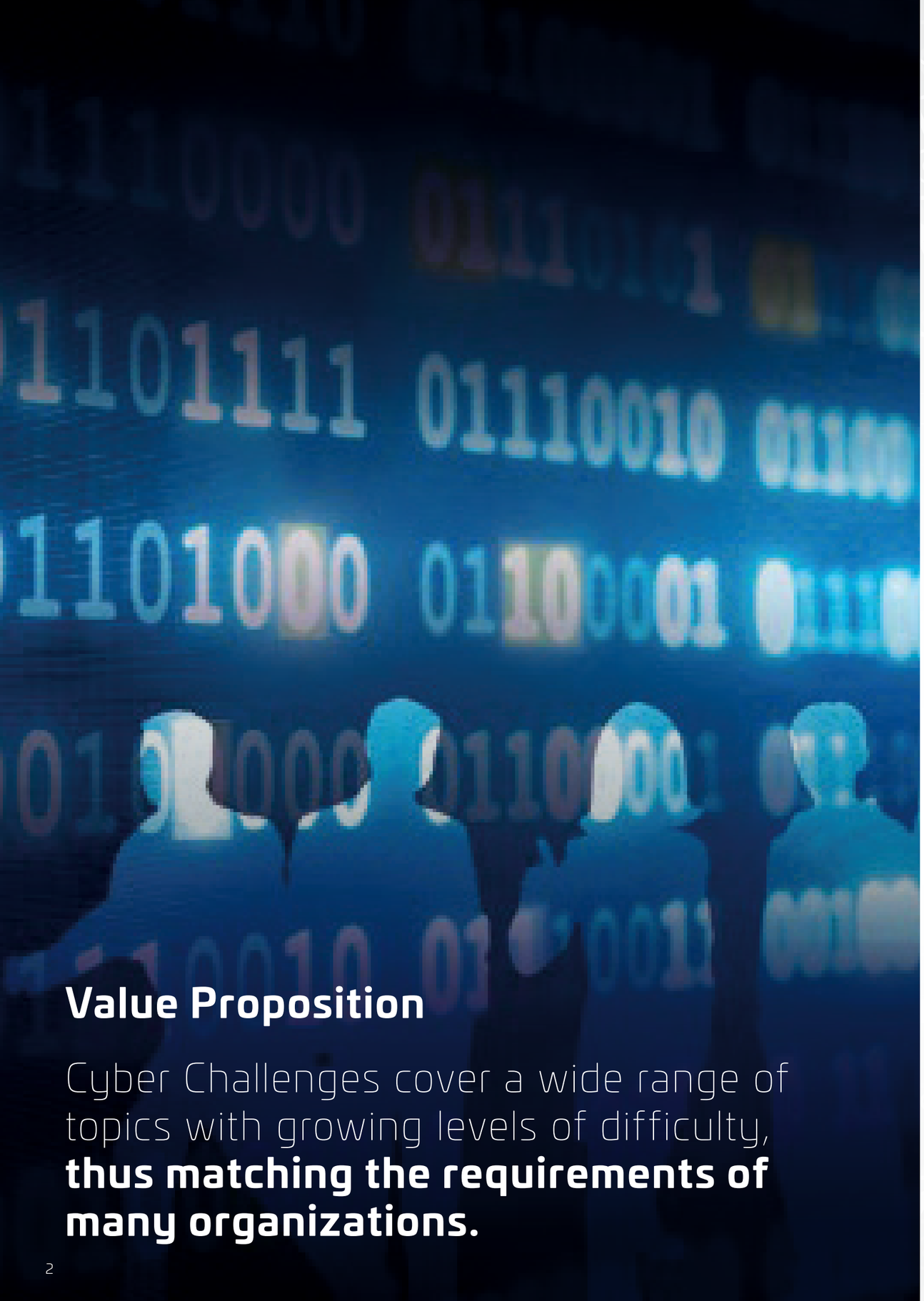
thalesgroup.com

THALES

diateam®

military & civil cybersecurity solutions

Thales Cyber Range
Powered by diateam



Value Proposition

Cyber Challenges cover a wide range of topics with growing levels of difficulty, **thus matching the requirements of many organizations.**

Thales Cyber Range
Powered by diateam

MARKET CHALLENGES AND OPPORTUNITIES

Is your organisation ready for the next cyber-attack? Information systems are increasingly targeted by more and more stealth and destructive cyber-attacks, that must to be detected as early as possible while cybersecurity experts are more in demand than ever.

To defend systems against today's highly organised attackers and to adopt an effective cybersecurity posture, organisations need to meet a number of basic requirements:

- Their teams must be trained regularly to be ready to respond efficiently to sophisticated attacks.
- Their IT infrastructures must be made secure and resilient.
- Existing security guidelines and response procedures must be upgraded and tuned to the challenge.

THALES OFFER/PROPOSAL

To help organizations meeting such requirements, Thales and diateam provide Cyber Range, a fit-for-purpose cybersecurity simulation platform that supports training, testing and research and development needs, providing:

- Realistic simulation of networks and technologies.
- Skills development training and development for incident response teams and other staff.
- Capacity to evaluate guidelines and incident response procedures.
- Ways to challenge people and working environments.

Cyber Range platform can also be used to evaluate security products and architectures in a managed virtual environment that is completely independent from the organisation's operational processes without the risk of knock-on effects on day to day operations.

OUR CREDENTIALS

- Global Leader In Data Protection
- 56 Countries
- 65 000 Thales Employees
- 5 Centers Of Cybersecurity Supervision
- Products And « High Grade » Security Solutions for 50 Including Nato
- 1 Cert-Ist Computer Emergency Response Team
- 5 000 It & Cybersecurity Ingeneer European Leader In Cybersecurity

Why **Thales**

Thales offers a professional training programme, addressing the needs of the main cybersecurity related job roles.

The Cyber Range platform is the cornerstone of this training program.

Thales' Cyber Academy provides training to major government organisations, with the highest level of participant satisfaction.

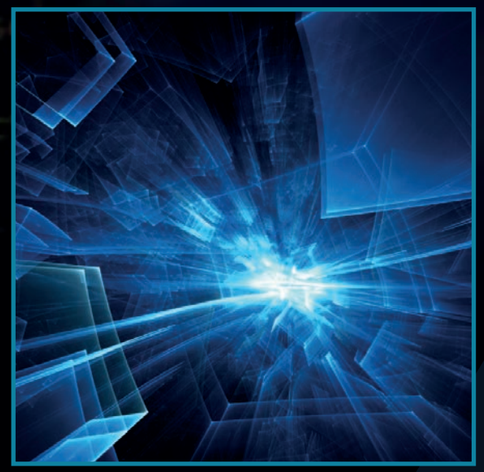
The Cyber Range platform is also used for Cyber Challenges in which your organization can take part to identify and recruit the best talents and to develop their skills.

Thales handles challenges' pratical aspects, including their technical preparation, supervision, candidates' performance analysis and pre-selection, and game debriefing.

Cyber Challenges cover a wide range of topics with growing levels of difficulty, thus matching the requirements of many organizations.

The Cyber Range is:

- **Scalable:** adapts to any user needs and to the Cyber Threat environment.
- **Realistic:** provides a full replication and simulation of your operational environment, including a traffic generator.
- **Versatile:** virtualizes of all types of IT network architectures and OT systems, with an extensive component library.
- **Hybrid:** connects virtual and real components, whether hardware and software.
- **Multiple training options:**
  - Red Team (hackers) vs. Blue Team (security personnel exercises)
  - Training using scenarios.
  - Large distributed exercises multiple connected Cyber Range platforms.
  - Cyber Challenges.



IN AN INCREASINGLY COMPLEX
DIGITAL WORLD
FACING CONSTANTLY **EVOLVING THREATS,**
REGULATION CHANGES AND **SKILLS SHORTAGE,**
EFFECTIVE AND TAILORED **CYBERSECURITY**
IS CRITICAL TO ADDRESSING BUSINESS **RISK** AND **OPERATIONAL**
RESILIENCE

Educate & Train

Realistic and adaptable attack scenarios

Prepare your teams for real life scenarios, even the most challenging ones.

- Use of standard attack scenarios in an incremental skills-building approach.
- Design of scenarios to meet the specific issues each organisation faces, with total user immersion.
- Expandable scenarios to take new threats into account.

Test & Analyse

Keeping pace with the latest threats

Connected with Thales' Cyber Threat Intelligence platform, Cyber Range is constantly updated with the latest threats as they emerge.

- New indicators of compromise added for even more realistic training experiences.
- Updates of system components (real or virtualized) put your security upgrades to the test.
- Continuous improvement of embedded detection and response capabilities in a safe environment.to take new threats into account.

Challenge & Motivate

Skills development and operational experience

Training exercises, with contents and methods tailored to specific requirements.

- For an optimal transfer ok incident supervision and response skills.
- For evaluating trainees' progress at the different stages of their education with cyber-challenges that help each trainee to test his skills.
- The use of organisation's own security components makes the training even more realistic and the people ready for their job.

Multiple training options:
Red Team (hackers) vs. Blue Team(security personnel exercises)
Training using scenarios.
Large distributed exercises multiple connected Cyber Range platforms.
Cyber Challenges.

Why Thales

- **Platform**
  - **Network virtualisation**
  - Mapping and reproduction of topologies specific to each organisation:
    - Libraries of virtual components.
    - IT/OT simulation capability.
    - Hybrid integration of real components/ interconnection with actual systems.
    - Solution scalability (from a few workstations to several thousands).
  - **Simulation of network activity**
    - Traffic generator to create legitimate and illegitimate traffic that can be injected into the system to reflect real life events.
    - Simulation of user profile traffic.
- **Content**
  - **Design and implementation of scenarios**
  - Scenario design tool.
  - Standard scenarios (training/basic).
  - Specific and advanced scenarios:
    - Sophisticated attacks scripting.
    - Tailored to specific business areas or architectures.
  - **Architecture library**
    - Standard architectures (IT/OT/web).
    - Specific architectures (defence, national ID cards, communication network, etc.).
  - **Enhanced user experience**
    - Specific building blocks.
    - Malware package.
    - Trainees supervision.
- **Services**
  - **Updates**
    - Malware package updates.
    - Scenario updates.
    - On-demand design of new scenarios with Cyber Threat Intelligence.
  - **Training**
    - Basic cybersecurity modules.
    - Advanced cybersecurity modules.
  - **Other**
    - Through life support and security maintenance.
    - Cyber challenges.
    - Product and/or solution testing.
    - Configuration testing.
    - Architecture testing and performance simulation.

350 Longwater Avenue,
Green Park, Reading
RG2 6GF
United Kingdom

Amanda Widdowson TC&C (UK):
+44 (0)7583 419027
amanda.widdowson@uk.thalesgroup.com
or
Centralised Cyber Consultancy:
cyber@uk.thalesgroup.com